

SECURITY - *Now ...more than ever!*

Cyber Security - Disaster Recovery - Continuity of Government



DTI eSecurity News – Public WiFi Safety

Where are WiFi 'Hot Spot' Locations?



WiFi hotspots are wireless networks that exist virtually everywhere. Airports, hotels, train stations, coffee shops, and many other places offer free WiFi. Many people use these hotspots without

thinking twice about others that may also be connected for reasons other than just surfing the web. Even though you may have security on your laptop, tablet, or smartphone; it does not mean the WiFi you are connecting to is secure.

What Are Public WiFi Dangers?



When connecting to the internet, there are many dangers. There are even more dangers when one connects to a Public WiFi network. Many public WiFi networks are not secure and are accessible by everyone.

- Other users may be able to unknowingly monitor or watch your internet activity.
- Public connections may not be encrypted.
- Without encryption, eavesdroppers can access your personal data.
- "Free WiFi" connections may have been set up by malicious individuals in an effort to steal your information.
- Eavesdropping is a very real possibility when connected to a public WiFi.

Tips to Stay Safe While Using Public WiFi



Most people have WiFi in their house and freely surf the net whenever they want. This freedom makes us feel comfortable. Sometimes we forget that the outside world is not as safe. Before you connect to a public WiFi, remember these tips:

- Keep your device or machine updated with the latest security software, operating system, web browser and apps.
- Don't assume that your connection to WiFi is secure. Many hotspots don't encrypt information you send when using their WiFi.
- When using public wireless networks, don't log into accounts that contain personal information, especially financial accounts.
- If a site looks suspicious, do not log into it. Check the spelling of the URL and if the URL address matches the business name that was given to you.
- Be careful when connecting to WiFi networks, called "free WiFi", because they might not be legitimate.
- In most cases, your cellular 3G/4G connection is more secure than a WiFi connection.
- Do not allow your devices to automatically connect to WiFi. Simply turn off the automatic connect feature and manually connect to WiFi instead.

Produced in part from resource [MS-ISAC](#)



Visit the [eSecurity](#) Extranet website for previous issues of

eSecurity Newsletters

Questions or comments?

E-mail us at esecurity@state.de.us